# BPA Policy 434-1

# Cyber Security Program

## Information Technology

## Table of Contents

## 434-1.1 Purpose & Background

This policy sets forth requirements and responsibilities for the Bonneville Power Administration Cyber Security Program (CSP) that protects both Information Technology and grid operations cyber systems. The implementation of this policy shall focus on reduction of risk while remaining consistent with obligations under relevant external regulations (see Authority section below) chiefly Department of Energy orders and directives, and the *Federal Information Security Management Act* and also including provisions to allow implementation of requirements of the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) standards pursuant to the Energy Policy Act of 2005 (Pub. L. 109-58).

Elements of this policy may provide evidence of compliance with NERC CIP, however this policy is not intended solely to be a NERC CIP policy.

## 434-1.2 Policy Owner

The BPA Chief Information Security Officer (CISO) is the owner of this policy.

## 434-1.3 Applicability

This policy is applicable to all personnel who use, access, modify, manage, maintain or operate IT or Grid IT equipment, including Transmission-owned or -managed cyber systems.

## 434-1.4 Terms & Definitions

Refer to *National Institute of Standards and Technology* (*NIST) Interagency Report (IR) 7298 Revision 1, Glossary of Key Information Security Terms* for additional definition related to cyber security, but not unique to this policy. The NIST IR 7298 Rev 1 includes most of the current terms & definitions used in NIST information security publications and those in the *CNSS Instruction No. 4009, National Information Assurance (IA) Glossary.*

NIST Special Publications and Federal Information Processing Standards contain the definitions for key terms used in the implementation of the IT risk management framework and the *Federal Information Security Management Act.*

Refer to *NERC Glossary of Terms Used in NERC Reliability Standards* for additional definition related to critical infrastructure protection, but not unique to this policy. The NERC Glossary of Terms Used in NERC Reliability Standards includes most of the current terms & definitions used in NERC CIP publications.

1. Administrator. The BPA Administrator. As the CEO of a Power Marketing Administration under the U.S. Department of Energy (DOE), the BPA Administrator is head of a DOE departmental element and a member of senior DOE management.

2. Annual. Occurring within a calendar year, (January 1 through December 31) with no more than 15 months between the events required by external standards.

3. Authorizing Official (AO). An authorizing official (AO) is a federal official with authority to formally assume responsibility for operating a cyber system at an acceptable level of risk

to BPA operations (including mission, functions, image, or reputation), BPA assets, or individuals.

4. Chief Information Officer (CIO). An official with overall responsibility for IT procurement, maintenance and operations including the selection and designation of the senior agency information security officer.

5. Chief Information Security Officer (CISO) / BPA Senior Agency Information Security Officer (SAISO). The official who ensures the development and maintenance of information security policies, procedures, and control techniques to address all applicable statutory requirements. Pursuant to FISMA, (§ 3544 (a)(3)(A)), the BPA CISO is the senior agency information security official responsible for carrying out CIO responsibilities under the statute and to act as the authorizing official designated representative.

6. Chief Technical Officer (CTO). The CTO is responsible for BPA Enterprise Architecture for the life-cycle management of information, information resources and related IT investments to maximize investments in information technology and ensure information technology is aligned with strategic goals. The CTO is responsible for the BPA Information Technology Architecture.

7. Cyber System: IT equipment or collections of IT equipment; any technology system (or collections thereof) capable of sending, receiving, or storing electronic data. Synonyms: GridIT, IT, information system, cyber asset, IT system. Examples: computing servers, user workstations, remote terminal units, phasor measurement units, network routers and switches, etc.

8. Information Owner (IO) (aka: Information Steward). Official with operational authority for specified BPA information (including responsibility for establishing controls for its generation, collection, processing, dissemination, storage and disposal); generally a business unit manager or designate.

9. Information System Owner (ISO). An official responsible for the overall procurement, development, integration, modification, or operation and maintenance of one or more cyber systems, including identifying and documenting in the system security plan (SSP): the operation of the information system; unique threats to the information system; and any special protection requirements identified by the information system owner, for each information system for which he or she is responsible.
    a. Establishing, documenting, and maintaining a role-based access model
    b. Approving, granting, and revoking access based on the principle of “least privileged”
    c. Tracking owners and users of shared access accounts
    d. Performing and reporting periodic reviews of access lists
    e. Ensure cyber security testing is performed in a manner that reflects production with minimal impact to operations
    f. Developing and maintaining Contingency-Recovery plans, pursuant to this policy
    g. Ensuring annual recovery and integrity testing of backup media

h. Ensuring compliance with all other controls set forth in these policies

i. Act as the subject matter expert representatives

j. Reviewing and retaining (for three calendar years) all records of granting, changing, or revocation (to include date) of physical and cyber access

k. Ensuring individuals with access to Critical Cyber Assets (CCAs) comply with all relevant NERC CIP requirements

l. Reviewing and updating all user access quarterly

m. Documenting the results of all user access review activity

10. Information System Security Officer (ISSO) / System Security Manager (SSM). Individual responsible to the ISO, IO and AO for maintaining an adequate operational security for one or more cyber systems. The SSM typically has the detailed technical knowledge and expertise required to manage the security aspects of the cyber system and is generally assigned responsibility for the day-to-day security operations.

11. Information Technology (Title 40 US Code, Section 11101):

    a. with respect to an executive agency means any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency, if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency that requires the use—

       (i) of that equipment; or

       (ii) of that equipment to a significant extent in the performance of a service or the furnishing of a product;

    b. includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources;

12. Privileged User. Any user who has been granted system administrator or network administrator, e.g. super-user access or root-level access, or has authority to alter the security controls or overall security configuration of a cyber system.

13. System Life Cycle. An examination of a system or proposed system that addresses all phases of its existence to include system conception inception, design and development, production and/or construction, distribution, operation, maintenance and support, retirement, phase-out and disposal. At BPA four domains span multiple phases of the life cycle.

14. North American Electric Reliability Corporation (NERC): The Federal Energy Regulatory Commission (FERC) appointed Electric Reliability Organization (ERO), responsible for development of the reliability standards for the Bulk Electric System (BES).

15. Critical Infrastructure Protection (CIP): The specific set of reliability standards, developed by NERC, pertaining to the physical and cyber security of BES critical assets. Commonly referred to as “NERC CIP.

16. CIP Exceptional Circumstance: A situation that involves or threatens to involve one or more of the following, or similar, conditions that impact safety or BES reliability: a risk of injury or death; a natural disaster; civil unrest; an imminent or existing hardware, software, or equipment failure; a Cyber Security Incident requiring emergency assistance; a response by emergency services; the enactment of a mutual assistance agreement; or an impediment of large scale workforce availability.

## 434-1.5 Policy

All BPA Information and Information Systems shall adhere to the provisions specified within FISMA, and further clarified within the following sections.

Management of all BPA-owned or –managed cyber systems must conform to the detailed requirements set forth under the BPA Cyber Security Program Plan, as currently amended.

A. **Assignment of Information System Owner:** All devices that meet the federal definition of IT under title 40 US code shall have an Information System Owner assigned and be included in the inventory of a system security plan as approved by the BPA Office of Cyber Security. Information System Owners will be designated in writing and will be responsible for implementation of all provisions in this policy. An emphasis will be given to implementation of real time automated capability for monitoring vulnerabilities, configuration management, asset management and security event logs.

B. **Cyber Security Risk Management:** A cyber security risk management program must be implemented and maintained to identify, evaluate, reduce, and accept security risk to BPA for all BPA cyber systems. The risk management program will consist of a method to categorize systems based on potential threat and impact to BPA missions, evaluate existing compensating controls, and manage exceptions identified through the program.

C. **Security Assessment and Authorization:** Processes must be in place to ensure adequate security assessment and formal risk determinations or decisions for all BPA information and cyber systems. The AO is formally responsible for accepting risk to the agency and providing Authority To Operate (ATO) for all cyber systems. All systems must be incorporated into the BPA security risk management framework, based on each system’s security category.

   Implementation of BPAs’ cyber and cyber security systems must meet these objectives:

   1. Periodically assess the security controls in organizational cyber systems to determine if the controls are effective in their application.
   2. Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational cyber systems.
   3. Authorize the operation of organizational cyber systems and any associated cyber system connections.

4. Monitor cyber system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

D. **Access Control:** Controls for both physical and electronic access must be provided for all personnel, devices and processes before granting any privileges within, or access to BPA cyber systems. Access controls for all BPA cyber systems must be implemented based on the principles of least-privilege and separation of duties.

E. **Awareness and Training:** Security awareness and training must be provided for all personnel with authorized access to cyber systems that support BPA mission functions, pursuant to this policy.

F. **Audit and Accountability**: All cyber systems that support BPA mission functions must incorporate auditing and accountability capabilities commensurate with each cyber system's security category.

G. **Configuration and Change Management:** Configuration and Change Management must be performed for all cyber systems that support BPA mission functions commensurate with each cyber system's security category. The Configuration and Change Management program must be implemented in a manner to track and manage all system changes, in order to reduce the risk of impact to BPA's missions.

H. **Contingency Planning:** Contingency planning must be an integral part of each cyber system's operational profile, commensurate with each system's security category.

I. **Continuous Monitoring:** FISMA directs heads of agencies to place all cyber systems under real time, continuous monitoring. In addition, BPA shall ensure the cyber security program applies a continuous assessment model to all security assessments and cyber system assessments.

J. **Identification and Authentication**: Identification and authentication controls must be commensurate with each cyber system's security category and must be provided for all personnel, devices and processes with authorized access to cyber systems that support BPA mission functions.

K. **Incident Response:** Incident response, i.e., incident handling and management, must be provided for all cyber systems that support BPA mission functions. BPA's specific approach to declaring and responding to CIP Exceptional Circumstances is described in Bonneville Power Administration Manual, Policy 21 and Dispatch Standing Order 136.

L. **Maintenance:** Structured maintenance programs must be in place for all cyber systems that support BPA mission functions, commensurate with each system's status in the BPA Systems Life Cycle (SLC) standard and its security category.

M. **Media Protection:** Media protection must be provided for all cyber systems that support BPA mission functions, commensurate with each cyber system's security category.

N. **Physical and Environmental Protection**: Physical and environmental protection must be provided for all cyber systems that support BPA mission functions, commensurate with each system's security category.

O. **Planning:** BPA must develop, document, periodically update, and implement security plans for their cyber systems that describes the security controls in place or planned for the cyber systems and the rules of behavior for individuals accessing the cyber systems.

P. **Personnel Security**: Personnel security programs must be in place for all personnel who have authorized access to cyber systems that support BPA mission functions, commensurate with each cyber system's security category.

Q. **System and Services Acquisition**: BPA prioritizes system and service acquisition activities to ensure that corrective actions identified in required annual FISMA reporting are incorporated into the capital planning process to deliver maximum security in a cost-effective manner. Funding high-priority security investments supports BPA's objective of maintaining appropriate security controls, both at the enterprise and system levels, commensurate with levels of risk and data sensitivity.

R. **System and Communication Protection**: System and communication protections must be provided for all cyber systems that support BPA mission functions, commensurate with each cyber system's security category. The systems and communication protections must be incorporated into an overall BPA strategy that implements the defense-in-depth security principle.

S. **System and Information Integrity**: System and information integrity programs must be provided for all cyber systems that support BPA mission functions, commensurate with each system's security category.

## 434-1.6 Policy Exceptions

Exceptions (to include NERC CIP related Technical Feasibility Exceptions) are defined as any non-conformity of programs, processes, or technologies as they relate to the requirements established within this policy and supporting standards.

All exceptions must be documented within thirty days of identification, and submitted no later than sixty days prior to compliance deadlines for approval by the Chief Information Security Officer (CISO). Documentation of all existing and terminated exceptions shall be maintained and tracked as compliance artifacts.

## 434-1.7 Responsibilities

A. **BPA Authorizing Official (AO)**

Responsibilities: grants formal Authority To Operate for information systems according to the BPA security authorization process. Authorizing Officials may, as needs warrant, appoint one or more AO Designated Representatives to act on their behalf. The AO exercises inherent U.S. government authority and must be a federal employee. The AO must have authority to oversee the budget and business operations of information systems within the BPA. The AO at BPA is a formal delegation available in Section IV of the Cyber Security Program, *Letters of Delegation and Designation*. The BPA AO function is accomplished through the Chief Operating Officer. The AO is the only individual at BPA that can accept risk.

B. **BPA Chief Information Security Officer (CISO) / BPA Senior Agency Information Security Officer (SAISO)**

Responsibilities: develops and maintains the BPA cyber security program and all supporting governance and standards documentation. The CISO is the authorizing official designated representative and the senior agency information security officer with statutory authority and responsibility. The CISO facilitates external and internal information security reviews, and coordinates site visits that support federal and DOE oversight and audits. The CISO provides an independent assessment of all NIST security controls for governance, compliance and oversight, and specific direction, guidance and assistance in order to correct deficiencies. The CISO provides technical testing and control assessment to the FERC governance and compliance office. For information security matters, the CISO serves as the CIO's primary liaison to the agency's AO, information owners, and information system owners. The CISO develops and maintains BPA's information security program to ensure effective implementation and maintenance of required information security policies, procedures, and control techniques. Federal requirements for cyber security are interpreted solely by the CISO. The CISO acts as the AODR.

C. **BPA Authorizing Official Designated Representative**

Responsibilities: The Authorizing Official Designated Representative (AODR) is an organizational official that acts on behalf of an AO to coordinate and conduct the required day-to-day activities associated with the security authorization process. The BPA Authorizing Official Designated Representative is delegated and empowered by the AO to make decisions with regard to the planning and resourcing of the security authorization process, approval of the security plan, approval and monitoring the implementation of plans of action and milestones, and the assessment and/or determination of risk.

D. **Information Owners (IO)**

Responsibilities: Official responsible for determining and declaring the sensitivity of the information created, processed, stored, transferred, or accessed on the information system. Information Owners advise the ISO of any special protection requirements of the information. IOs are responsible to approve and review access to cyber assets and to inform the authorizing official of business or mission risks regarding cyber security vulnerabilities or controls. IOs are responsible to understand how cyber security risks affect the devices and systems that impact their mission.

E. **Information System Owner (ISO)**

Responsibilities: Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of one or more information systems. The ISO is responsible for operating an information system on behalf of one or more Information Owners, who specify the data access requirements and conditions which meet the business requirements supported by the system. The ISO coordinates all aspects of the system from initial concept, through development, to implementation and system maintenance. The ISO is responsible for the selection, development, maintenance and effective implementation of all applicable security controls for each information system. ISOs are responsible to ensure the IO knows their functional responsibilities and the general cyber security posture of the equipment and systems that support the IO mission functions and sub functions.

F. **Information System Security Officer (ISSO) / System Security Manager (SSM)**

Responsibilities: Responsible for identifying and documenting in the system security plan (SSP): the operation of the information system; unique threats to the information system; and any special protection requirements identified by the ISO, for each information system for which he or she is responsible.

G. **Common Control Provider**

Responsibilities: The common control provider is an individual, group, or organization responsible for the development, implementation, assessment, and monitoring of common controls (i.e., security controls inherited by information systems). Common control providers are responsible for: (i) documenting the organization-identified common controls in a security plan (or equivalent document prescribed by the organization); (ii) ensuring that required assessments of common controls are carried out by qualified assessors with an appropriate level of independence defined by the organization; (iii) documenting assessment findings in a security assessment report; and (iv) producing a plan of action and milestones for all controls having weaknesses or deficiencies. Security plans, security assessment reports, and plans of action and milestones for common controls (or a summary of such information) is made available to the ISO inheriting those controls after the information is reviewed and approved by the senior official or executive with oversight responsibility for those controls.

H. **NERC CIP Senior Manager:**

Responsibilities: BPA shall designate a Senior Manager with overall responsibility and authority for managing the implementation and compliance with NERC CIP standards. Any change to this designation must be documented within thirty calendar days of the effective change. The NERC CIP Senior Manager will ensure that Bulk Electric System (BES) cyber systems, as defined by NERC, have a formally appointed IO and ISO as required by this policy and that all BES assets that meet the federal definition of IT are managed in conformance with this policy and that any conflicts with Department of Energy directives or the BPA Cyber Security Program Plan (CSPP) are resolved or documented as an exception.

## 434-1.8 Standards & Procedures

Control families, and the control requirements governing implementations of each control family, are specified in the CSPP and the BPA Information Technology Architecture or elsewhere as indicated.

Cyber Security Program Standards are available on the BPA Office of Cyber Security Intranet Site.

Applicable standards are located or referenced within the Bonneville Information Technology Architecture (BITA) published on the Chief Technical Officer (CTO) SharePoint site.

System Life Cycle (SLC) processes, procedures, document templates, and examples are published on the CTO's SLC SharePoint site.

The Cyber Security Program Plan and associated standards and requirements are located on the BPA Office of Cyber Security Website.

Other procedures and internal requirements to meet specific requirements of federal regulation and NERC CIP standards are located in other documentation as noted in this policy.

## 434-1.9 Performance & Monitoring

The GOISSP shall provide quarterly management reporting to the CISO and NERC CIP Senior Manager with regard to agency compliance with this policy.

## 434-1.10 Authorities & References

A. E-Government Act of 2002, Public Law 107-347, Title III, Federal Information Security Management Act of 2002 (FISMA), P.L. 107-307, 44 U.S.C. § 3541, et seq. as amended.

B. DOE Order 205.1B, Department of Energy Cyber Security Management Program

C. North American Electric Reliability Corporation – Critical Infrastructure Protection (NERC-CIP) standards

D. FIPS-199 Security Category

E. FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems

F. Government Performance Results Act of 1993 (GPRA), P.L. 103-62, as amended.

## 434-1.11 Review

This policy shall be reviewed by the policy owner annually for relevant purpose, content, currency, effectiveness, and metrics.

## 434-1.12 Revision History

| Version | Issue Date | Description of Change |
|---|---|---|
| 1.0 | 12/8/2014 | Initial creation by Mike Harris from GOISSM Policy doc. |
| 2.0 | 1/30/2015 | Revisions for Cyber Security Program inclusions |
| 3.0 | 3/2/2015 | Grammatical corrections from RFC, moved a few blocks to appropriate sections, added CIP Exceptional Circumstances – Mike Harris |